Bayerisches Landesamt für
Datenschutzaufsicht

Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

Muster 5: Arztpraxis

Hinweis:
Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. *Verantwortlicher*. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die *wesentlichen* Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

Kurzbeschreibung der Arztpraxis

Ein Arzt hat eine Hausarztpraxis auf dem Land mit fünf ArzthelferInnen/MFAs, einer Putzkraft und einem Sicherstellungsassistenten. Die Arztpraxis betreibt eine kleine Webseite mit Hilfe eines Content Management Systems, auf dem online Termine angefragt werden können. Ein externer Dienstleister betreut die Webseite und die Praxis-IT. Die Datenverarbeitung bezüglich der Patientendaten erfolgt auf eigenen Computern und Servern innerhalb der Praxis.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohn- und Gehaltsabrechnung der Mitarbeiter
- Verarbeitung von Patientendaten zur Behandlung
- Verarbeitung von Patientendaten zur Abrechnung über die KVB bzw. PVS
- Betrieb der Webseite mit der Online-Terminbuchungsmöglichkeit

Wesentliche DS-GVO-Anforderungen für die Arztpraxis

A Datenschutzbeauftragter (DSB)
Muss ein DSB vom Arzt benannt werden?
☐ ja
☒ nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten
Ist ein solches Verzeichnis erforderlich?
☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
☐ nein

C Datenschutz-Verpflichtung von Beschäftigten
Ist eine solche Verpflichtung durchzuführen?
☒ ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
☐ nein

D Information- und Auskunftspflichten
Bestehen irgendwelche Informationspflichten?
☒ ja (insb. in der Praxis durch Flyer/Aushang sowie auf der Webseite in der Datenschutzerklärung)
☐ nein

E Löschen von Daten
Gibt es eine Anforderung zur Datenlöschung?
☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
☐ nein

F Sicherheit
Müssen die Daten besonders gesichert werden?
☒ ja (da sensible Daten verarbeitet werden, sind weitere Schutzmaßnahmen erforderlich)
☐ nein

G Auftragsverarbeitung
Ist ein Vertrag zur Auftragsverarbeitung notwendig?
☒ ja (mit dem IT-Betreuer, der die Webseite und die Praxis-IT betreut)
☐ nein

H Datenschutzverletzungen
Müssen bestimmte Vorfälle gemeldet werden?
☒ ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
☐ nein

I Datenschutz-Folgeabschätzung (DSFA)
Muss eine DSFA in Arztpraxis durchgeführt werden?
☐ ja
☒ nein (da auch bei Gesundheitsdaten nicht immer ein hohes Risiko bei der Datenverarbeitung besteht)

J Videoüberwachung (VÜ)
Besteht eine Ausschilderungspflicht bezüglich VÜ?
☐ ja
☒ nein (da keine Videoüberwachung durchgeführt wird)

ⓘ Erläuterungen zu den Anforderungen

A Datenschutzbeauftragter (DSB)

In der Arztpraxis findet in aller Regel keine umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten statt, die zu einer Benennungspflicht führt. Es ist daher ein DSB nur zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig beschäftigt" ist z. B. die Arzthelferin. „Nicht ständig beschäftigt" ist dagegen bspw., wer als Putzkraft theoretisch Daten zur Kenntnis nehmen kann.

⇨ **DSK-Kurzpapier Nr. 12:** *www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf*

B Verzeichnis von Verarbeitungstätigkeiten

Arztpraxen, gehen mit gesundheitsbezogenen Daten um und müssen ein Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇨ **BayLDA Muster-Verzeichnis für kleine Arztpraxen:** *www.lda.bayern.de/media/muster_5_arztpraxis_verzeichnis.pdf*
⇨ **DSK-Kurzpapier Nr. 1:** *www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf*
⇨ **DSK-Muster-Verzeichnis allgemein:** *www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf*

C Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

⇨ **BayLDA Info-Blatt zur Verpflichtung:** *www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf*

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich sind (z. B. Flyer, Aushang, Homepage). Die betroffenen Personen haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

⇨ **DSK-Kurzpapier Nr. 6:** *www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf*
⇨ **DSK-Kurzpapier Nr. 10:** *www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf*

E Löschen von Daten

Sobald keine gesetzliche Grundlage (z. B. Aufbewahrungspflicht für Behandlungsunterlagen) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. Dies ist in der Regel bspw. der Fall, wenn nach Abschluss der Behandlung 10 Jahre vergangen sind.

⇨ **DSK-Kurzpapier Nr. 11:** *www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf*

F Sicherheit

Um die sensiblen Patientendaten bei der Verarbeitung zu schützen, sind neben Standardmaßnahmen weitere Maßnahmen zu treffen. Als Standardmaßnahmen zählen u.a. aktuelle Betriebssysteme, Passwortschutz, regelmäßige Backups und Virenscanner. Daneben sollte das Praxisverwaltungssystem von einem Recherche-PC getrennt werden und der Zugriff auf Patientendaten nur denjenigen in einem Zugriffs- und Berechtigungskonzept gewährt werden, die diesen für ihre Arbeit benötigen. Das Onlineterminbuchungsformular muss Ende-zu-Ende und transportverschlüsselt werden.

⇨ **BayLDA-Kurzpapier Nr. 1:** *www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf*

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. IT-Wartung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

⇨ **DSK-Kurzpapier Nr. 13:** *www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf*
⇨ **BayLDA-Formulierungshilfe zum Vertrag:** *www.lda.bayern.de/media/muster_adv.pdf*

H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung eines Arztbriefes), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

⇨ **BayLDA-Kurzpapier Nr. 8:** *www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf*
⇨ **BayLDA-Online-Service zur Meldung:** *www.lda.bayern.de/de/datenpanne.html*

I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

⇨ **DSK-Kurzpapier Nr. 5:** *www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf*

J Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich.

⇨ **DSK-Kurzpapier Nr. 15:** *www.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf*